

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-196240
 (43)Date of publication of application : 11.07.2003

(51)Int.Cl. G06F 15/00
 H04L 9/32

(21)Application number : 2001-400547
 (22)Date of filing : 28.12.2001

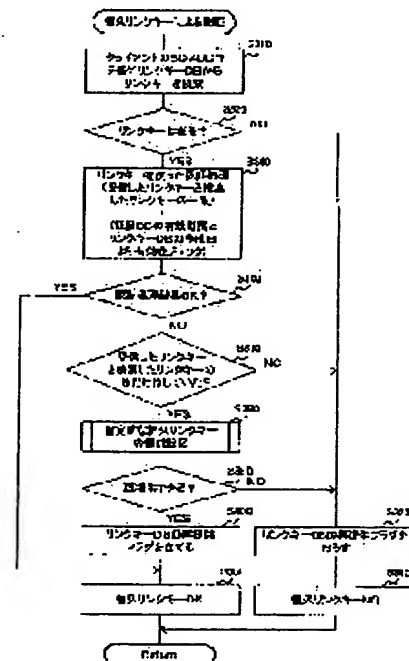
(71)Applicant : BROTHER IND LTD
 (72)Inventor : MATSUDA MAKOTO

(54) SERVICE PROVIDER, SERVICE PROVIDING SYSTEM, SERVICE PROVIDING PROGRAM, COMPUTER READABLE RECORDING MEDIUM WITH ITS PROGRAM RECORDED

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a service providing device capable of flexibly dealing with a service request.

SOLUTION: In this service providing system, a server 20 executes authentication processing to a client 10 based on a permanent link key acquired from a client 10 and a permanent link key registered in its own authentication DB (S340), and even when the client 10 is not authenticated by the permanent link key within the term of validity (S350: NO), as long as the client 10 is authenticated by the permanent key beyond the term of validity (S370: YES), a service is temporarily provided under a prescribed condition (S390: YES). Thus, it is possible to flexibly deal with the service request, and it is possible for a user side to easily use the service.



LEGAL STATUS

[Date of request for examination] 26.06.2003
 [Date of sending the examiner's decision of rejection]
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

BEST AVAILABLE COPY

[0007]

Further, especially in the service providing device of claim 1, the temporary service providing means provides a temporary service even when the client device is not authenticated by the authenticating means, as long as the client device is a client device authenticated by the authenticating means in the past.

[0054]

As shown above, in this service providing system, the server 20 executes authentication processing to the client 10 based on a permanent link key acquired from a client 10 and a permanent link key registered in its own authentication DB (S340), and even when the client 10 is not authenticated by the permanent link key within the term of validity (S350: NO), as long as the client 10 is authenticated by the permanent link key beyond the term of validity (S390: YES), a service is temporarily provided under a prescribed condition (S390: YES). Thus, it is possible to flexibly deal with the service request, and it is possible for a user side to easily use the service.

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-196240
(P2003-196240A)

(43) 公開日 平成15年7月11日 (2003.7.11)

(51) Int.Cl.	識別記号	FI	キーワード(参考)
G06F 15/00	330	G06F 15/00	330C 5B085
H04L 9/32		H04L 9/00	675Z 5J104

審査請求 未請求 請求項の数7 OL (全9頁)

(21) 出願番号 特願2001-400547(P2001-400547)

(22) 出願日 平成13年12月28日 (2001.12.28)

(71) 出願人 000005267

ブラザー工業株式会社

愛知県名古屋市長区瑞穂区苗代町15番1号

(72) 発明者 松田 誠

愛知県名古屋市長区瑞穂区苗代町15番1号
ブラザー工業株式会社内

(74) 代理人 100082500

弁理士 足立 勉 (外1名)

Fターム(参考) 5B085 AE03 AE04 BC02

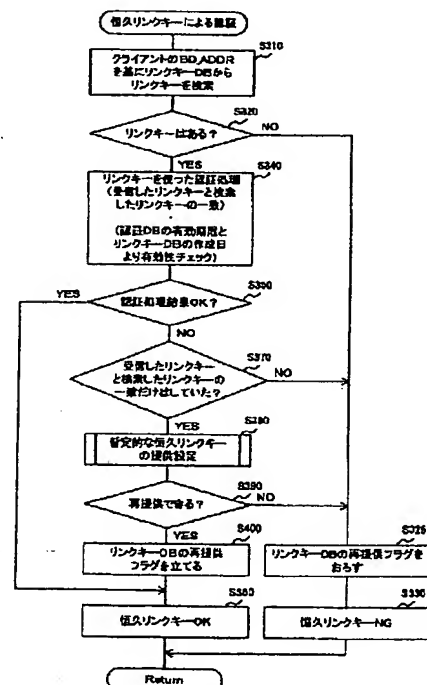
5J104 AA07 KA02 PA07

(54) 【発明の名称】 サービス提供装置、サービス提供システム、サービス提供プログラムおよび当該プログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 サービス提供装置において、サービス要求に対して柔軟な対応ができるようにする。

【解決手段】 本実施例のサービス提供システムにおいて、サーバ20は、クライアント10から取得した恒久リンクキーと自己の認証DBに登録されている恒久リンクキーとに基づいて、クライアント10に対する認証処理(S340)を行った結果、有効期限内の恒久リンクキーによってクライアント10が認証されない場合であっても(S350:NO)、有効期限切れの恒久リンクキーによって認証される場合には(S370:YES)、所定の条件の下で、暫定的にサービスを提供する(S390:YES)。これにより、サービス要求に対する柔軟な対応が実現され、利用者側がサービスを利用し易くなる。



【特許請求の範囲】

【請求項1】照合情報を記憶する記憶手段と、クライアント装置から入手した認証情報と前記記憶手段に記憶された照合情報とに基づき、前記クライアント装置の認証を行う認証手段と、該認証手段によりクライアント装置が認証された場合に、サービスを提供するサービス提供手段とを備えたサービス提供装置であって、前記認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が、過去に前記認証手段により認証されたクライアント装置である場合は、暫定的なサービスを提供する暫定サービス提供手段を更に備えたことを特徴とするサービス提供装置。

【請求項2】前記記憶手段は、前記照合情報として、現在の及び過去の照合情報を記憶しており、前記サービス提供手段は、前記認証手段を介して、前記クライアント装置から入手した認証情報と前記現在の照合情報とに基づいてクライアント装置が認証された場合にサービスを提供するとともに、前記暫定サービス提供手段は、前記認証手段によりクライアント装置が認証されない場合であっても、前記認証情報と前記過去の照合情報とに基づいて当該クライアント装置が認証された場合は、暫定的なサービスを提供することを特徴とする請求項1に記載のサービス提供装置。

【請求項3】前記暫定サービス提供手段に基づく暫定的なサービスを提供する際に、所定の情報をクライアント装置に通知する通知手段を備えたことを特徴とする請求項1又は請求項2に記載のサービス提供装置。

【請求項4】請求項1乃至請求項3の何れか1項に記載のサービス提供装置において、当該装置は複数のサービスを提供できるものであり、前記暫定サービス提供手段に基づく暫定的なサービスの提供可否が、該サービスごとに設定されていることを特徴とするサービス提供装置。

【請求項5】照合情報を記憶する記憶手段と、クライアント装置から入手した認証情報と前記記憶手段に記憶された照合情報とに基づき、前記クライアント装置の認証を行う認証手段と、該認証手段によりクライアント装置が認証された場合に、サービスを提供するサービス提供手段とを備えたサービス提供装置、としてコンピュータを機能させるためのプログラムであって、更に、前記認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が、過去に前記認証手段により認証されたクライアント装置である場合は、暫定的なサービスを提供する暫定サービス提供手段としてコンピュータを機能させるためのサービス提供プログラム。

【請求項6】請求項5に記載のサービス提供プログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項7】クライアント装置と、

照合情報を記憶する記憶手段と、クライアント装置から入手した認証情報と前記記憶手段に記憶された照合情報とに基づき、前記クライアント装置の認証を行う認証手段と、該認証手段によりクライアント装置が認証された場合に、サービスを提供するサービス提供手段とを備えたサービス提供システムであって、

前記認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が、過去に前記認証手段により認証されたクライアント装置である場合は、暫定的なサービスを提供する暫定サービス提供手段を更に備えたことを特徴とするサービス提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、クライアント装置が認証された場合に、サービス提供を行うサービス提供装置、サービス提供システム、サービス提供プログラム及び当該プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】従来より、クライアント装置が認証された場合にサービス提供を行うサービス提供装置においては、パスワードやリンクキー（後に後述する）などを入力させ、その入力されたパスワードやリンクキーが正規のものであるか否かを判断することによって認証処理を行っている。

【0003】しかし、印刷サービス等もネットワーク化に伴い、利用する人が増加する傾向にあるため、中にはパスワードやリンクキーを何らかの方法によって盗みとり、不当にサービスの提供を受けようとする者がいる虞がある。この様な不安に対処するために、管理者としては、パスワードやリンクキーに有効期限を設けたり、定期的にそれらを変更することによってセキュリティを強化することが考えられる。

【0004】

【発明が解決しようとする課題】しかしながら、セキュリティを強化するために、パスワードやリンクキーに有効期限を設けたり、定期的にそれらを変更することは有効であるが、有効期限が切れたことや、パスワードやリンクキーの変更に気付かず、以前のパスワードやリンクキーを用いてサービスを要求したユーザーには、サービスが提供されない。

【0005】このようなユーザは、元々正規のユーザであるにも拘わらず、不当にサービスを受けようとする者を排除するために、突然サービスの提供が認められないといった不利益を与えていた。本発明はこうした課題を背景としてなされたものであり、サービス提供装置、サービス提供システム、サービス提供プログラム及び当該プログラムを記録したコンピュータ読み取り可能な記録媒体において、セキュリティを確保しつつ、サービス要求に対して柔軟な対応ができるようにすることを目的と

する。

【0006】

【課題を解決するための手段及び発明の効果】上記課題を解決するためになされた請求項1記載のサービス提供装置においては、認証手段が、クライアント装置から入手した認証情報と、記憶手段に記憶された照合情報とに基づいて、クライアント装置の認証処理を行い、その結果、クライアント装置が認証された場合に、サービス提供手段がサービスを提供する。

【0007】そして特に請求項1記載のサービス提供装置においては、認証手段によりクライアント装置が認証されない場合であっても、当該クライアント装置が過去に認証手段により認証されたクライアント装置である場合、暫定サービス提供手段が、暫定的なサービスを提供する。

【0008】つまり、請求項1のサービス提供装置によれば、クライアント装置が認証されない場合であっても、サービス利用側は、暫定的ではあるがサービスを受けることができることとなる。即ち、サービス要求に対して柔軟な対応ができ、利用者側がサービスを利用し易くなるという効果を奏する。

【0009】サービス提供を暫定的なものとするのは、例えば、サービス提供を一定期間に限定したり、サービス提供の回数を限定したりするなど、サービスを提供するための条件を定めておくことで実現できる。また、過去に認証手段により認証されたクライアント装置であるかどうかを判断できるようにするには、例えば、請求項2に記載の様にサービス提供装置を構成すればよい。

【0010】即ち、請求項2に記載のサービス提供装置においては、記憶手段に、照合情報として、現在の及び過去の照合情報を記憶させており、サービス提供手段を、認証手段を介して、クライアント装置から入手した認証情報と現在の照合情報とに基づいてクライアント装置が認証された場合にサービスを提供するように構成している。そして、暫定サービス提供手段については、認証手段によりクライアント装置が認証されない場合であっても、認証情報と過去の照合情報とに基づいて当該クライアント装置が認証された場合は、暫定的なサービスを提供するよう構成している。

【0011】この様に構成された請求項2に記載のサービス提供装置によれば、過去に認証手段により認証されたクライアント装置であるかどうかを判断することができる。ところで、暫定サービス提供手段によるサービス提供は暫定的なものであり、いつまでもそのサービス提供を受けることはできない。そこで、請求項3に記載の様に、暫定的なサービスを提供する際、通知手段に、所定の情報をクライアント装置に通知させるようにするとよい。この様にすれば、サービス利用側に対して注意を促すことができ、サービスがより利用しやすくなる。

【0012】また、当該サービス提供装置が複数のサービスを提供できるものである場合には、請求項4に記載の様に、暫定サービス提供手段に基づく暫定的なサービスの提供可否を、サービス毎に設定しておくといふ。この様にすれば、サービス提供の運用により柔軟性を持たせることができる。

【0013】なお、請求項5のサービス提供プログラム、および請求項6のコンピュータ読み取り可能な記録媒体によれば、コンピュータを、請求項1のサービス提供装置と同様に機能させることができ、この装置と同様の効果を得ることができる。また、請求項7に記載のサービス提供システムによれば、請求項1のサービス提供装置と同様の効果を得ることができる。

【0014】

【発明の実施の形態】以下に、本発明の一実施例を図面と共に説明する。図1は、一実施例としてのサービス提供システム1の構成を示す図である。このサービス提供システムは、後述するリンクキーを記憶するための記憶部12を有するクライアント装置（以下、「クライアント」という）10と、サーバ装置（以下、「サーバ」という）20とから構成されている。

【0015】サーバ20は、図2に示す様に、CPU30、RAM40、ROM50等からなるコンピュータ、入力装置60、表示装置70、通信装置80、印刷装置90で構成されており、ファクシミリ装置やプリンタ装置などとしての機能を備えた複合装置であって、プリントサービスやFAXサービスなど、複数のサービスを提供できるものである。尚、サーバ20は、請求項の「サービス提供装置」に相当する。

【0016】CPU30は、制御部32、演算部34、データ比較部36などから構成されており、ROM50に格納されたプログラムに基づいて所定の処理を実行するものである。ROM50には、請求項の「サービス提供プログラム」を構成する、認証制御プログラム52やその他の動作プログラム54が格納されている。

【0017】RAM40には、認証データベース(DB)42、サービスDB44、リンクキーDB46、各種動作バッファ48などの記憶領域が確保されている。認証DB42は、データ項目として、図3(a)に示す様に、“認証の種類”、“認証の有無”、“有効期限”、“無効時の対応(回数)”および“無効時の対応(期限)”を有するデータベースである。

【0018】またサービスDB44は、データ項目として、図3(b)に示す様に、“サービス”、“認証の種類”、“PINコード”および“恒久リンクキーの種類”を有するデータベースである。この“サービス”は、サーバ20が提供可能なサービスである。

【0019】またリンクキーDB46は、データ項目として、図3(c)に示す様に、“恒久リンクキー”、“恒久リンクキーの種類”、“BDアドレス”、“生成

日”、“再提供回数”、“再提供有効期限”および“再提供フラグ”を有するデータベースである。リンクキーDB46(具体的にはRAM40)は、請求項の「記憶手段」として機能するものであり、“恒久リンクキー”が、請求項の「照合情報」に相当する。

【0020】入力装置60は、外部から入力操作を行うための入力部62と、入力部62に入力された情報をCPU30に入力する入力制御部64とを備えている。また、表示装置70は、CPU30からの表示データを一旦蓄える表示制御バッファ72と、表示制御バッファ72に蓄えた表示データに基づく画像を表示部74に表示させる表示制御部76とを備えている。

【0021】通信装置80は、CPU30と通信データを送受する通信ポート82と、アンテナ84を用いて無線通信を制御する無線制御部86とを備え、クライアント10と通信可能に構成されている。クライアント10およびサーバ20は、Bluetooth方式の無線通信によりデータの送受信を行う通信機器(BT通信機器)であり、他のBT通信機器(本実施形態では、Bluetooth方式の通信に対応したクライアント装置10)との間で、Bluetooth方式の無線通信を行う。Bluetooth方式の通信では、通信開始時のリンクレイヤにおいて、リンクキーと呼ばれる秘密鍵を用いて接続認証が行われることにより、誤接続防止等のセキュリティが図られている。

【0022】BT通信機器では、通信相手となる他のBT通信機器毎に、そのBDアドレスと、2機器間で利用されるリンクキーとをペアにして記憶し管理するようになっている。例えば、本実施例のサーバ20においては、リンクキーDB46に、クライアント10のBDアドレスとリンクキーとをペアにして登録している。ここで、2機器間で利用されるリンクキーには、半固定的なリンクキーとしてのユニットキー及びコンビネーションキーと、一時的なリンクキーとしての初期化キーとがある。ユニットキーおよびコンビネーションキーは、機能的には同じものであるが、前者は単一のBT通信機器の情報から生成されるものであるのに対し、後者は2つのBT通信機器の情報を組み合わせて生成される点で異なる。

【0023】通信相手についての半固定的なリンクキー(即ち、ユニットキー又はコンビネーションキー、以下、恒久リンクキーという)が既に設定されている場合には、そのリンクキーを用いて接続認証が行われるが、恒久リンクキーが設定されていない場合には、暫定的なリンクキーである初期化キーを生成する。

【0024】ここで、初期化キーの生成方法について説明する。まず、初期化キーを生成しようとする2つのBT通信機器(以下、機器A及び機器Bとして説明する)において、接続要求を受けた側の機器Bが、当該機器Bで発生した乱数を接続要求側の機器Aに送信する。ま

た、各機器のBDアドレスは、通信の初期段階において交換されており、2機器間で周知のパラメータとなっている。

【0025】そして、機器Aは、当該機器AのBDアドレスと、当該機器AのPINコードと、機器Bで発生した乱数とから、初期化キー生成のための演算を行い、初期化キーを算出する。同様に、機器Bも、機器AのBDアドレスと、当該機器BのPINコードと、当該機器Bで発生した乱数とから、初期化キー生成のための上記演算を行い、初期化キーを算出する。尚、初期化キーを生成する場合、クライアント10側においては当該クライアント10のPINコードを入力する必要がある。

【0026】一方、2つのBT通信機器間の接続認証は、それぞれのBT通信機器で通信相手について設定されているリンクキーが一致するか否かを判定することにより行われる。ここで、リンクキーが一致するか否かの判定方法について説明する。

【0027】接続認証を行おうとする2つのBT通信機器(以下、機器C及び機器Dとして説明する)において、認証要求を受けた側の機器Dが、当該機器Dで発生した乱数を認証要求側の機器Cに送信する。また、各機器のBDアドレスは、通信の初期段階において交換されており、2機器間で周知のパラメータとなっている。

【0028】そして、機器Cは、当該機器CのBDアドレスと、機器Dについて設定されているリンクキーと、機器Dで発生した乱数とから、接続認証のための演算を行い、SRESと呼ばれるパラメータを算出する。同様に、機器Dも、機器CのBDアドレスと、機器Cについて設定されているリンクキーと、当該機器Dで発生した乱数とから、接続認証のための上記演算を行い、SRESを算出する。そして、機器Cは、当該機器Cで算出したSRESを機器Dへ送信する。一方、機器Dは、当該機器Dで算出したSRESと、機器Cから受信したSRESとが一致するか否かを判定する。

【0029】ここで、機器Dが、2つのSRESが一致したと判定すると、接続認証が成立する。このように、接続認証では、セキュリティ確保のため、それぞれのBT通信機器で通信相手について設定されているリンクキーが一致するか否かを、リンクキー自体を送信することなく判定するようになっている。

【0030】なお、印刷装置90は、CPU30から印刷データを受信する通信ポート92と、CPU30から受信した印刷データを一時的に蓄える印刷制御バッファ94と、印刷データに基づいて印刷動作を制御して印刷部96から印刷物を出力させる印刷制御部98とから構成されている。

【0031】以上の様に構成されたサーバ20において、ROM50に格納されたプログラムに基づいてCPU30が実行する処理につき、以下に説明する。図4は、クライアント10からサービスの要求を受信した

後、サーバ20において行われる処理を示すフローチャートである。

【0032】図4に示すように、サーバ20は、サービス要求を受けると、その要求された”サービス”に基づいて、サービスDB44から”認証の種類”を検索し（S10）、その結果得られた”認証の種類”に基づいて、認証DB42から”認証の有無”を検索する（S20）。”認証の有無”は、認証を行うかどうかを判断するためのデータ項目であり、認証DB42の検索の結果得られた”認証の有無”に基づいて、認証処理を行うかどうかを判断する（S30）。

【0033】その結果、認証処理を行わないものと判断した場合には（S30：NO）、直ちにサービス提供処理に移行するが（S80）、認証処理を行うものと判断した場合には（S30：YES）、認証処理を行う（S40）。なお、認証処理（S40）の詳細については、後述する（図5参照）。

【0034】認証処理（S40）を終えると、認証処理の結果が「OK」かどうかを判断し（S50）、「OK」でない場合は（S50：NO）、サービスの提供を行わない。一方、認証処理の結果が「OK」である場合には（S50：YES）、リンクキーDB46の”再提供フラグ”が立っているかどうかを判断する（S60）。”再提供フラグ”は、リンクキーの有効期限が切れた場合において、暫定的にサービスの提供を許可するとき立てられるフラグである。

【0035】”再提供フラグ”が立っていない場合には（S60：NO）、そのままサービス提供処理に移行するが（S80）、”再提供フラグ”が立っている場合には、この後に提供するサービスが暫定的なサービス提供であることをクライアント10のユーザに通知して（S70）、サービス提供を行う（S80）。

【0036】なお、CPU30は、S70の処理を実行することによって請求項の「通知手段」として機能し、S80の処理を実行することによって請求項の「サービス提供手段」として機能する。図5は、サーバ20で行われる認証処理を示すフローチャートである。

【0037】認証処理において、サーバ20は、クライアント10に対して恒久リンクキーによる認証要求を行い（S110）、その後、クライアント10が恒久リンクキーを返信してきたかどうかを判断する（S120）。クライアント10から恒久リンクキーが返信されない場合には（S120：NO）、恒久リンクキーを新規に作成する（S130）。そして、恒久リンクキーの新規作成が問題なく行われたかどうかを判断し（S140）、所定の問題があった場合には（S140：NO）、認証処理の結果を「NG」として（S150）、当該認証処理を終了する。一方、その作成が問題なく行われた場合には（S140：YES）、恒久リンクキーによる認証処理を行う（S160）。なお、”恒久リン

クキーの新規作成”の詳細については後述する（図6参照）。

【0038】クライアント10から恒久リンクキーが返信された場合には（S120：YES）、直ちに恒久リンクキーによる認証処理を行う（S160）。クライアント10から送られる恒久リンクキーは、請求項の「認証情報」に相当するものである。なお、恒久リンクキーによる認証処理については後述する（図7参照）。

【0039】恒久リンクキーによる認証処理（S160）を終えると、その結果が「OK」であるかどうかを判断し（S170）、「OK」であれば（S170：YES）、認証結果を「OK」とし（S180）、その後、当該認証処理を終了する。一方、「OK」でなければ（S170：NO）、認証結果を「NG」とし（S150）、その後、当該認証処理を終了する。

【0040】図6は、”恒久リンクキーの新規作成”処理を示すフローチャートである。サーバ20は、要求を受けた”サービス”に基づいて、サービスDB44から”PINコード”を検索し、それに基づいて初期化キーを作成すると共に（S210）、クライアント10から初期化キーを受信する（S220）。そして、作成した初期化キーに基づいて、受信した初期化キーを認証する（S230）。即ち、初期化キーに基づいて、当該”サービス”への接続についての認証（初期認証という）を行うのである。

【0041】次に、初期認証の結果が「OK」かどうかを判断し（S240）、「OK」でない場合には（S240：NO）、直ちに当該恒久リンクキー新規作成処理を終了するが、「OK」である場合には（S240：YES）、要求を受けた”サービス”に基づいて、”サービスDB44に登録してある”恒久リンクキーの種類”を検索し、その”恒久リンクキーの種類”が”ユニットキー”かどうかを判断する（S250）。

【0042】その判断の結果、検索された”恒久リンクキーの種類”がユニットキーである場合には（S250：YES）、ユニットキーを生成し（S260）、一方、”恒久リンクキーの種類”がユニットキーでない場合には（S250：NO）、コンビネーションキーを生成する（S270）。そして、生成したリンクキーを、リンクキーDB46に登録する（S280）。

【0043】図7は、サーバ20において行われる”恒久リンクキーによる認証”処理を示すフローチャートである。この認証処理において、サーバ20は、クライアント10の”BDアドレス”に基づいて、リンクキーDB46からリンクキーを検索し（S310）、リンクキーがあるかどうかを判断する（S320）。

【0044】ここで、リンクキーがない場合には（S320：NO）、リンクキーDB46の再提供フラグをおろすとともに（S325）、恒久リンクキーによる認証の結果を「NG」として（S330）、当該”恒久リン

クキーによる認証処理”を終了する。

【0045】一方、リンクキーがある場合には（S320：YES）、そのリンクキーを用いた認証処理を行う（S340）。この認証処理（S340）の結果が「OK」となるには、受信したリンクキーとリンクキーDB46に登録されているリンクキーとが一致していること、およびリンクキーDB46に登録されているリンクキーが有効期限内であることが必要である。リンクキーが有効期限内かどうかについては、認証DB42の”有効期限”、リンクキーDB46の”生成日”および現在の日付に基づいて判断される。

【0046】この様な認証処理（S340）を終え、その結果が「OK」かどうかを判断し（S350）、「OK」である場合には（S350：YES）、恒久リンクキーによる認証の結果を「OK」とし（S360）、当該恒久リンクキーによる認証処理”を終了する。

【0047】ところで、上記の認証処理の結果が「OK」でない場合には（S350：NO）、クライアント10から受信したリンクキーと、リンクキーDB46を検索して得られたリンクキーとが一致していたかどうかを判断する（S370）。この判断の結果、両リンクキーが一致していない場合には（S370：NO）、S330に移行するが、両リンクキーが一致している場合には（S370：YES）、リンクキーDB46に登録されている恒久リンクキーの有効期限が切れただけであると判断されるので、当該恒久リンクキーに関して、”暫定的な恒久リンクキーの提供設定”を行う。”暫定的な恒久リンクキーの提供設定”とは、恒久リンクキーの有効期限が切れている場合に、所定の条件の下で、暫定的に、その恒久リンクキーを有効なものとするためのものであるが、その詳細については後述する（図8参照）。

【0048】”暫定的な恒久リンクキーの提供設定”（S380）を終えると、暫定的なサービス提供（以下、「再提供」という）をすることができるかどうかを、その処理結果に基づいて判断する（リンクキーDB46の再提供回数が0回でなく、かつ、リンクキーDB46の再提供有効期限が0日でない場合にのみ、再提供が許可される）（S390）。そして、再提供できない場合には（S390：NO）、S330に移行するが、再提供できる場合には（S390：YES）、リンクキーDB46において当該”恒久リンクキー”に対応する”再提供フラグ”を立て（S400）、その後、S360に移行する。

【0049】なお、CPU30は、S340～S360の処理を実行することにより、請求項の「認証手段」として機能し、S370～S400の処理を実行することにより、請求項の「暫定サービス提供手段」としての機能する。また、リンクキーDB46には、有効期限内の

恒久リンクキーおよび有効期限切れの恒久リンクキーの両方が記録されているのであるが、有効期限内の”恒久リンクキー”が、請求項における「現在の照合情報」に相当し、有効期限を過ぎた”恒久リンクキー”が、請求項における「過去の照合情報」に相当するものである。

【0050】図8は、”暫定的な恒久リンクキーの提供設定”処理を示すフローチャートである。本処理においては、”再提供フラグ”が立っているかどうかを、リンクキーDB46を検索して判断する（S510）。”再提供フラグ”が立っている場合には（S510：YES）、リンクキーDB46の”再提供回数”を1減らし（S520）、直ちに”暫定的な恒久リンクキーの提供設定”処理を終了する。

【0051】一方、”再提供フラグ”が立っていない場合には（S510：NO）、S10で検索された”認証の種類”に対応する”無効時の対応（回数）”が「NG」となっているかどうかを、認証DB42を検索して判断する（S530）。ここで、「NG」である場合には（S530：YES）、リンクキーDB46の”再提供回数”を「0」とする（S540）と共に、”再提供有効期限”を「0」とし（S550）、当該”暫定的な恒久リンクキーの提供設定”を終了する。

【0052】また、認証DB42の”無効時の対応（回数）”が、「NG」でない場合には（S530：NO）、リンクキーDB46の”再提供回数”に、認証DB42の”無効時の対応（回数）”のデータを設定し（S560）、そして、認証DB42の”無効時の対応（期限）”が「NG」かどうかを判断する（S570）。その結果、認証DB42の”無効時の対応（期限）”が「NG」である場合には（S570：YES）、S550に移行し、「NG」でない場合には（S570：NO）、リンクキーDB46の”再提供有効期限”に、認証DB42の”無効時の対応（期限）”のデータを設定し（S580）、その後、当該”暫定的な恒久リンクキーの提供設定”を終了する。

【0053】つまり、認証DB42の”無効時の対応（回数）”および”無効時の対応（期限）”とサービスDB44の”サービス”とは、”認証の種類”に基づいて関連づけられ、これにより、サーバ20が提供可能な”サービス”ごとに暫定的なサービス提供の可否（条件）が設定されている。そして、その条件の下で、暫定的なサービスの提供が行われるのである。

【0054】以上の様に、本実施例のサービス提供システムにおいて、サーバ20は、クライアント10から取得した恒久リンクキーと自己の認証DB42に登録されている恒久リンクキーとに基づいて、クライアント10に対する認証処理（S340）を行った結果、有効期限内の恒久リンクキーによってクライアント10が認証されない場合であっても（S350：NO）、有効期限切れの恒久リンクキーによって認証される場合には（S3

70: YES)、所定の条件の下で、暫定的にサービスを提供する(S390: YES)。これにより、サービス要求に対する柔軟な対応が実現され、利用者側がサービスを利用し易くなる。

【0055】また、暫定的なサービスを提供する際（S60：YES）、所定の情報、即ち暫定的なサービス提供であることをクライアント10のユーザに通知して注意を促すため、サービスがより利用しやすくなる。また、暫定的なサービスの提供可否を、サービス毎に設定しているため、サービス提供システムを柔軟性に運用することができる。

【００５６】以上、本発明の一実施例について説明したが、本発明は上記実施例に限定されるものではなく、種々の態様をとることができる。例えば、上記実施例では、暫定的なサービスを提供する条件として、回数および期間に制限を設けたが、これに限られるものではない。サービスの内容に応じて、回数のみを制限するようにしてもよいし、また期間のみに制限を設けてもよい。

【0057】また、上記実施例では、Bluetooth方式により、クライアント10とサーバ20とが無線通信を行うものとして説明したが、これに限られるものではない。更に、上記実施例では、リンクキーの一致及びリンクキーの有効性（有効期限内であること）に基づいて認証処理を行い（S40）、共に条件を満たす場合に認証処理OKとする例を挙げて説明したが、リンクキーの有効性（有効期限内であること）については、検討しない構成としても良い。つまり、リンクキーの一致不一致に基づいて認証処理を行う構成としても良い。この場合、過去のリンクキー（過去の照合情報）をリンクキーDBに記憶しておき、現在のリンクキー（現在の照合情報）と一致しなくても、過去のリンクキーと一致す

る場合に、暫定的なサービスを提供する構成となる。このような構成によれば、管理者によって定期的、あるいは不規則に認証の種類を変えたとしても、その変更前のユーザに対しては、少なくとも暫定的なサービスが提供されることとなるため、セキュリティの向上とユーザに対する利便性とをうまく両立させることが可能である。

【図面の簡単な説明】

【図１】 一実施例としてのサービス提供システム１の構成を示す図である。

【図2】 サーバの構成を示すブロック図である。

【図3】 (a)は認証データベースの内容、(b)はサービスデータベースの内容、(c)はリンクキーデータベースの内容を示す図である。

【図4】 サービス要求を受けた後にサーバで行われる処理を示すフローチャートである。

【図5】 サーバで行われる認証処理を示すフローチャートである。

【図6】 サーバで行われる恒久リンクキーの新規作成処理を示すフローチャートである。

【図7】 サーバで行われる恒久リンクキーによる認証処理を示すフローチャートである。

【図8】 サーバで行われる暫定的な恒久リンクキーの提供設定処理を示すフローチャートである。

【符号の説明】

1…サービス提供システム

10…クライアント装置

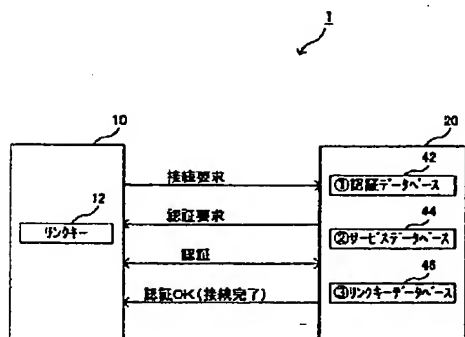
20...サーバ装置 30...CPU

4 0...RAM 5 0...ROM

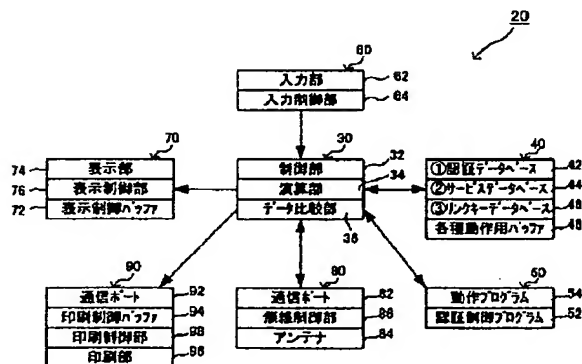
4 2…認証DB 4 4…サービスDB

46...リンクキーDB

【図 1】



【図2】



【図3】

(a) 認証データベース

認証の種類	認証1	認証2	認証3
認証の有無	行わない	行う	行う
有効期限	NG	14日	30日
無効時の対応(回数)	NG	NG	+M回
無効時の対応(期限)	NG	NG	10日

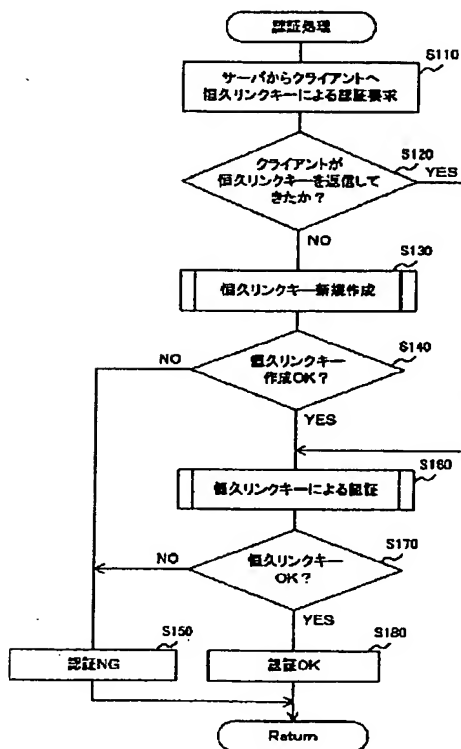
(b) サービスデータベース

サービス	サービスA(グリッド)	サービスB(FAX)	サービスC(***)
認証の種類	認証3	認証2	認証1
PINコード	***	なし	***
恒久リンクキーの種類	エディケーション	ユニット	コンビネーション

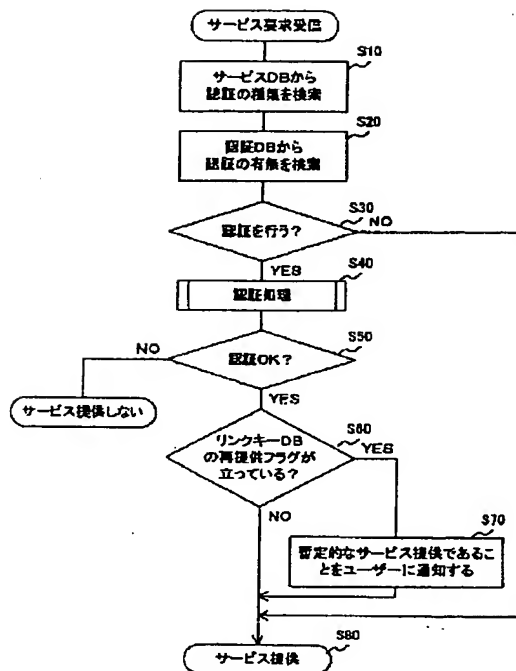
(c) リンキーデータベース

恒久リンクキー	リンクキー-1	リンクキー-2
恒久リンクキーの種類	コンビネーション	コンビネーション
EO_ADDR	*****	*****
生成日	***	***
再提供回数	0	M
再提供有効期限	0	10日
再提供フラグ	0	1

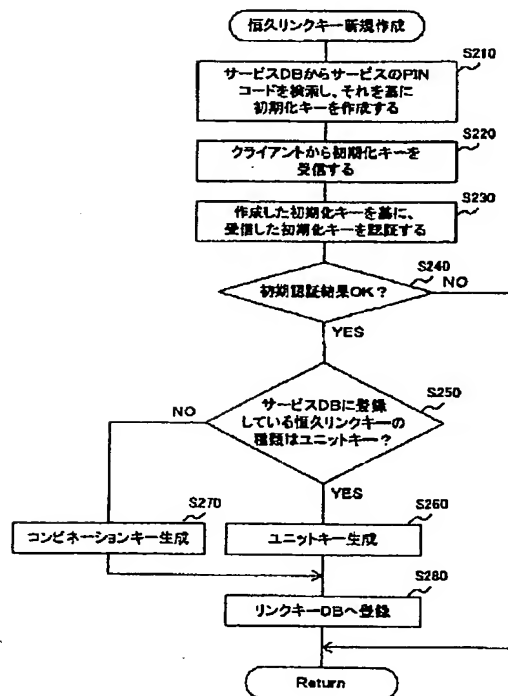
【図5】



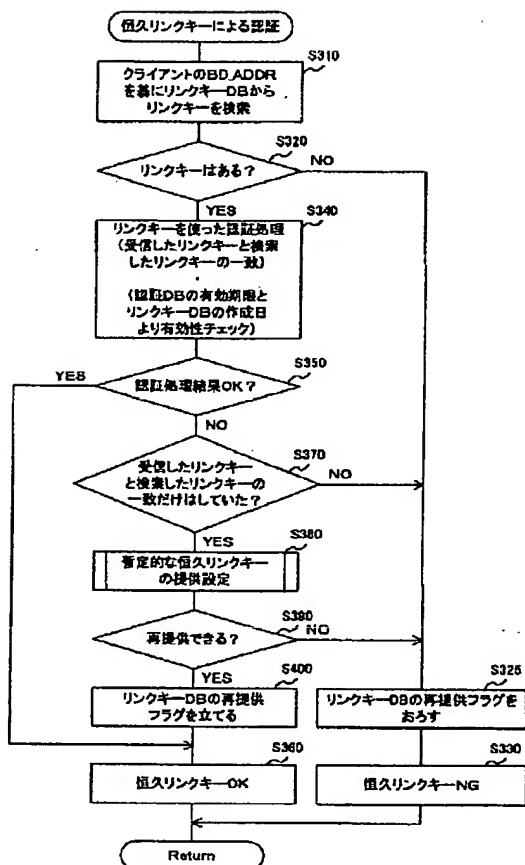
【図4】



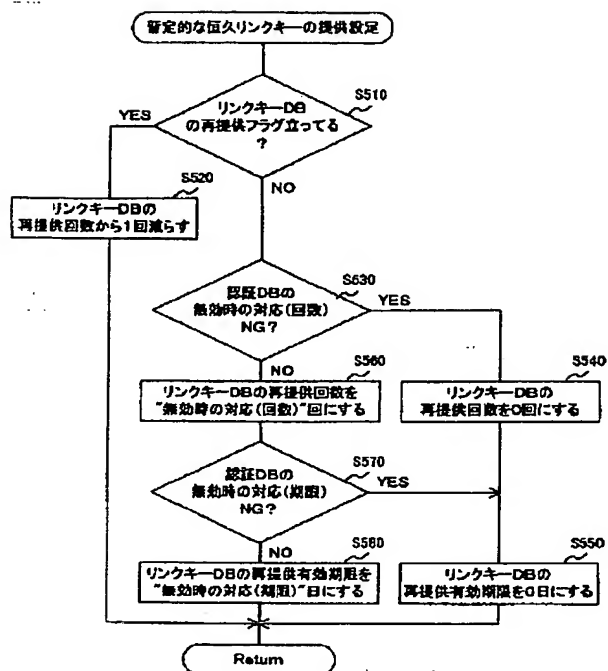
【図6】



【図7】



【図8】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.